Hong Kong Special Administrative Region who are fleeing oppression by the Government of the People's Republic of China.

(e) TERMINATION.—This section shall cease to have effect on the date that is 5 years after the date of the enactment of this Act.

SA 4241. Mr. MENENDEZ submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title XII, add the following:

Subtitle H—Combating International Cybercrime

SEC. 1291. DEFINITIONS.

In this subtitle:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations of the Senate;

(B) the Committee on Banking, Housing, and Urban Affairs of the Senate;

(C) the Committee on Foreign Affairs of the House of Representatives; and

(D) the Committee on Financial Services of the House of Representatives.

(2) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' means systems and assets, whether physical or virtual, that are so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on the security, economic security, public health, or safety of the United States.

(3) CYBERCRIME GROUP.—The term ''cybercrime group'' means any group practicing, or which has significant subgroups which practice, international cybercrime.

(4) INTERNATIONAL CYBERCRIME.—The term ''international cybercrime'' means unlawful activities involving citizens, territory, or infrastructure of at least 1 country that is intended—

(A) to disrupt the confidentiality, integrity, or availability of information systems for financial gain or in order to economically benefit a third party;

(B) to damage, delete, deteriorate, alter, or suppress information systems; or

(C) to distribute credentials, access codes, or similar data.

(5) MAJOR CYBERCRIME INCIDENT.—The term ''major cybercrime incident'' means an act of cybercrime, or a series of such acts, that—

(A) results in the death of, or bodily injury to, 1 or more United States citizens;

(B) results in economic loss to United States persons in excess of—

(i) $5,000,000 in any single act of cybercrime; or

(ii) $50,000,000 in a series of acts of cybercrime; or

(C) materially disrupts United States critical infrastructure.

(6) STATE SPONSOR OF INTERNATIONAL CYBERCRIME..—The term ''state sponsor of international cybercrime'' means a country, the government of which systematically—

(A) commits international cybercrime;

(B) supports, facilitates, encourages, or expressly consents to international cybercrime by third parties, including contractors, proxies, and affiliates; or

(C) fails to take reasonable steps to detect, investigate, or address cybercrime occurring within its territory or through the use of its infrastructure.

SEC. 1292. FINDINGS.

Congress finds the following:

(1) Information and communication technologies underpin the prosperity and national security of the United States. However, the widespread use of these technologies also poses serious risks. In particular, cybercrime (criminal activity using digital means) presents an acute and growing threat to the economic, strategic, and security interests of the United States and its allies and partners.

(2) Cybercriminals cause massive harm. According to National Institute of Standards and Technology estimates, in 2016, United States businesses lost between $167,900,000,000 and $770,000,000,000 to cybercrime, corresponding to between 0.9 percent and 4.1 percent of the total United States gross domestic product that year. The related risk and harm to public health and safety is incalculable and can only be expected to grow as digital technologies become more intertwined in daily life.

(3) Using a wide variety of tactics, cybercriminals—

(A) steal United States intellectual property and sensitive personal information;

(B) defraud United States businesses and citizens; and

(C) disrupt infrastructure critical to Americans' health and safety.

(4) The use of ransomware (malicious software that encrypts and thereby prevents access to data) until a ransom, often costing millions of dollars, is paid is a an especially destructive form of cybercrime.

(5) In 2021, ransomware groups—

(A) crippled or endangered some of the United States' most critical infrastructure, including water utilities, hospitals, meat packing plants, and a critical fuel pipeline; and

(B) extracted hundreds of millions of dollars in ransom from United States businesses and their insurers.

(6) United States allies and partners have also suffered major losses from cybercrime. Recent ransomware victims include Swedish supermarkets, Ireland's national health service, a leading European insurer, and a major German chemical manufacturer.

(7) The Council of Europe's Convention on Cybercrime, done at Budapest November 23, 2001, states, ''an effective fight against cybercrime requires increased, rapid and well-functioning international cooperation in criminal matters'' and requires parties to outlaw digital fraud, digital forgery, intellectual property theft through digital means, and offenses against confidentiality, integrity, and availability of computer data and systems, among other misconduct.

(8) In July 2021, the United Nations Group of Governmental Experts on Advancing responsible State behavior in cyberspace, which includes experts from the United States, Russia, and China, issued a report stating that countries are expected to ''take all appropriate and reasonably available and feasible steps to detect, investigate and address'' known cybercriminal activity emanating from within their borders.

(9) Certain nations, including China, Russia, Iran, and North Korea, ignore, facilitate, or directly participate in cybercrime as a matter of national policy.

(10) Russia is a global haven for cybercriminals, including ransomware groups responsible for attacks on fuel pipelines, meat packing plants, and supermarkets in the United States and in Europe in 2021. These gangs operate freely and with the Kremlin's tacit approval. By allowing cybercriminals to operate with impunity, Russia threatens international stability, undermines international institutions, and disregards international norms.

(11) The People's Republic of China uses cybercrime—

(A) to undermine United States' interests; and

(B) to victimize United States' businesses and government agencies.

(12) In July 2021, Secretary of State Blinken stated, ''The PRC's Ministry of State Security (MSS) has fostered an ecosystem of criminal contract hackers who carry out both state-sponsored activities and cybercrime for their own financial gain. ... These contract hackers cost governments and business billions of dollars in stolen intellectual property, ransom payments, and cybersecurity mitigation efforts, all while the MSS has them on its payroll.''.

(13) Cybercrime is central to North Korea's geopolitical strategy, helping the Kim Jong Un regime maintain its grip on power and providing essential resources for the country's nuclear weapons program.

(14) In February 2021, the Department of Justice indicted 3 North Korean military intelligence agents for a ''wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks, to steal and extort more than $1.3 billion of money and cryptocurrency from financial institutions and companies, to create and deploy multiple malicious cryptocurrency applications, and to develop and fraudulently market a blockchain platform.''.

(15) North Korean hackers are responsible for many of the most brazen cybercrime campaigns, including—

(A) the 2017 WannaCry global ransomware incident;

(B) the 2014 cyberattack on Sony Pictures; and

(C) the attempted theft of nearly $1,000,000,000 from the Central Bank of Bangladesh in 2016.

(16) The Iranian regime is a prolific sponsor of cybercrime. Hackers linked to Iran's Islamic Revolutionary Guard Corps target businesses, academic institutions, and research organizations around the world.

(17) In 2018, the Department of Justice indicted 9 Iranians for a coordinated campaign of cyber intrusions into computer systems belonging to 144 United States universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children's Fund.

SEC. 1293. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) all nations must take reasonable steps to stop cybercriminal activities from taking place within their territories or through their infrastructure;

(2) governments that tolerate, facilitate, or participate in cybercrime threaten the economic and national security of the United States, United States allies and partners, and the international community; and

(3) the rising threat of international cybercrime requires a robust, coordinated response from the United States Government, United States allies and partners, and the private sector—

(A) to prevent and counter international cybercriminal activity; and

(B) to impose significant and tangible costs on cybercriminal groups and on governments that tolerate, facilitate, or participate in cybercrime.

SEC. 1294. STATEMENT OF POLICY.

It shall be the policy of the United States—

(1) to prioritize efforts to counter international cybercrime in United States diplomatic, national security, and law enforcement activities related to cybersecurity and information communication technology;

(2) to cooperate with United States allies and partners to develop and implement strategies, policies, and institutions to address international cybercrime, including joint law enforcement efforts and efforts to develop effective international law and norms related to cybercrime control; and

(3) to identify and impose tangible costs on foreign governments that enable or engage in international cybercrime.

SEC. 1295. DESIGNATION OF STATE SPONSORS OF INTERNATIONAL CYBERCRIME.

(a) IDENTIFYING STATE SPONSORS OF INTERNATIONAL CYBERCRIME.—

(1) LIST OF STATE SPONSORS OF INTERNATIONAL CYBERCRIME.—Not later than 1 year after the date of the enactment of this Act, and not less frequently than annually thereafter, the Secretary of State shall—

(A) compile, or update, a list of countries that the Secretary has identified as state sponsors of international cybercrime; and

(B) make such list publicly available by publishing the list in the Federal Register and through other appropriate means.

(2) CONSULTATION.—In identifying state sponsors of international cybercrime pursuant to paragraph (1), the Secretary of State shall consult with the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the heads of other appropriate Federal agencies, and, to the extent the Secretary deems appropriate, officials of governments of countries that are allies or key partners of the United States.

(3) REMOVAL FROM LIST.—The identification by the Secretary that a country is a state sponsor of international cybercrime may not be rescinded after such country is included on the list described in paragraph (1)(A) unless the President submits to the Committee on Foreign Relations of the Senate, the Committee on Banking, Housing, and Urban Affairs of the Senate, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Financial Services of the House of Representatives—

(A) before the proposed rescission would take effect, a report certifying that—

(i) there has been a fundamental change in the leadership and policies of the government of such country;

(ii) such government is not a state sponsor of international cybercrime; and

(iii) such government has provided assurances that it will not engage in conduct in the future that would make such country a state sponsor of international cybercrime; or

(B) not later than 45 days before the proposed rescission would take effect, a report justifying the rescission and certifying that—

(i) the government of such country has not been a state sponsor of international cybercrime at any time during the preceding 18-month period; and

(ii) such government has provided assurances to the United States that the government will not engage in conduct in the future that would make such country a state sponsor of international cybercrime.

(4) PROHIBITION OF REMOVAL.—A rescission under paragraph (3) may not be made if Congress, not later than 45 days after receiving a report from the President under such paragraph, enacts a joint resolution stating, after the resolving clause, the following: ''That the proposed rescission of the identification of _____ as a state sponsor of international cybercrime, pursuant to the report submitted by the President to Congress on _____ is hereby prohibited.'', with the first blank filled in with the name of the applicable country and the second blank filled in with the appropriate date.

(b) RESTRICTION ON EXPORTS TO STATE SPONSORS OF INTERNATIONAL CYBERCRIME.—Section 1754 of the Export Controls Act of 2018 (50 U.S.C. 4813) is amended—

(1) by redesignating subsections (d), (e), and (f) as subsections (e), (f), and (g), respectively;

(2) by inserting after subsection (c) the following:

''(d) STATE SPONSORS OF INTERNATIONAL CYBERCRIME.—

''(1) COMMERCE LICENSE REQUIREMENT.—A license shall be required for the export, reexport, or in-country transfer of items, the control of which is implemented pursuant to subsection (a) by the Secretary, to a country if—

''(A) at the time of the proposed export, reexport, or in-country transfer of items, such country is identified as a state sponsor of international cybercrime on the list compiled or updated pursuant to section 1295(a)(1) of the National Defense Authorization Act for Fiscal Year 2021; and

''(B) the Secretary of State determines that the export, reexport, or in-country transfer of such items could materially enhance the ability of such country, or individuals or entities operating from its territory through its infrastructure, to commit, cause, or facilitate international cybercrime.

''(2) NOTIFICATION TO CONGRESS.—The Secretary of State shall include in the notification required under subparagraph (A)—

''(A) a detailed description of the items to be offered, including a brief description of the capabilities of any item for which a license to export, reexport, or in-country transfer the items is sought;

''(B) the reasons why the foreign country, person, or entity to which the export, reexport, or in-country transfer is proposed to be made has requested the items under the export, reexport, or in-country transfer, and a description of the manner in which such country, person, or entity intends to use such items;

''(C) the reasons why the proposed export, reexport, or in-country transfer is in the national interest of the United States;

''(D) an assessment of the ways in which the items proposed to be exported, reexported, or transferred in-country could be used for international cybercrime, and the likelihood that the items would be so used; and

''(E) an assessment of the potential harm to the United States or its allies if the items proposed to be exported, reexported, or transferred in-country were used for cybercrime.'';

(3) in subsection (f), as redesignated, by striking ''subsection (d)'' each place such term appears and inserting ''subsection (e)''; and

(4) in subsection (g), as redesignated, by striking ''subsection (d)'' each place such term appears and inserting ''subsection (e)''; and

(c) RESTRICTIONS ON MUNITIONS SALES TO STATE SPONSORS OF INTERNATIONAL CYBERCRIME.—Section 40 of the Arms Export Control Act (22 U.S.C. 2780) is amended—

(1) in the section heading, by adding at the end the following: ''**OR ACTS OF INTERNATIONAL CYBERCRIME**''; and

(2) by amending subsection (d) to read as follows:

''(d) STATE SPONSORS OF INTERNATIONAL TERRORISM OR INTERNATIONAL CYBERCRIME.—The prohibitions contained in this section apply with respect to a country if—

''(1) the Secretary of State determines that the government of such country has repeatedly provided support for acts of international terrorism, including any activity that the Secretary determines willfully aids or abets—

''(A) the international proliferation of nuclear explosive devices to an individual or group;

''(B) an individual or group in acquiring unsafeguarded special nuclear material; or

''(C) the efforts of an individual or group to use, develop, produce, stockpile, or otherwise acquire chemical, biological, or radiological weapons; or

''(2) at the time the transaction is proposed, such country is identified as a state sponsor of international cybercrime on the list compiled or updated pursuant to section 1295(a)(1) of the National Defense Authorization Act for Fiscal Year 2021.''.

(d) RESTRICTION ON FOREIGN ASSISTANCE TO STATE SPONSORS OF INTERNATIONAL CYBERCRIME.—Section 620A(a) of the Foreign Assistance Act of 1961 (22 U.S.C. 2371(a)) is amended to read as follows:

''(a) PROHIBITION.—The United States shall not provide any assistance under this chapter, the Food Peace Act [7 U.S.C. 1691 et seq.], the Peace Corps Act [22 U.S.C. 2501 et seq.], or the Export-Import Bank Act of 1945 [12 U.S.C. 635 et seq.] to any country if—

''(1) the Secretary of State determines that the government of such country has repeatedly provided support for acts of international terrorism; or

''(2) at the time the assistance is proposed to be provided, such country is identified as a state sponsor of international cybercrime on the list compiled or updated pursuant to section 1295(a)(1) of the National Defense Authorization Act for Fiscal Year 2021.''.

(e) ANNUAL COUNTRY REPORT ON INTERNATIONAL CYBERCRIME.—

(1) IN GENERAL.—Not later than April 30 of each year, the Secretary of State, in consultation with the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence, and the Director of the Central Intelligence Agency, shall submit a full and complete report to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives that includes—

(A) detailed assessments with respect to—

(i) each foreign country that, at the time of such submission, is identified as a state sponsor of international cybercrime on the list compiled or updated pursuant to subsection (a)(1);

(ii) any other foreign country that is materially involved or implicated in international cybercrime;

(B) all relevant information about the activities during the preceding year of any cybercrime group, and any umbrella organization under which such group falls, which was responsible for a major cybercrime incident during the 5-year period immediately preceding such submission;

(C) with respect to each foreign country from which the United States Government has sought cooperation during such 5-year period in the investigation or prosecution of a major cybercrime incident—

(i) the extent to which the government of the foreign country is cooperating with the United States Government in apprehending, convicting, and punishing the individual or individuals responsible for such incident; and

(ii) the extent to which the government of the foreign country is cooperating in preventing further acts of international cybercrime against the United States; and

(D) with respect to each foreign country from which the United States Government has sought cooperation during the previous 5 years in the prevention or disruption of activity that could lead to a major cybercrime

incident, the information described in paragraph (3)(B).

(2) ADDITIONAL PROVISIONS.—In addition to the information described in paragraph (1), the report required under such paragraph shall describe—

(A) with respect to paragraph (1)(A)—

(i) direct involvement in international cybercrime, if any, of each country that is the subject of such report;

(ii) significant support for international cybercrime, if any, by each country that is the subject of such report, including—

(I) political and financial support;

(II) technical assistance;

(III) the use of state infrastructure or personnel;

(IV) protection from detection, prosecution, or extradition, whether by action or inaction; and

(V) intelligence;

(iii) the extent of knowledge by the government of each country that is the subject of such report with respect to international cybercrime occurring within its territory or through the use of its infrastructure;

(iv) the efforts of each country that is the subject of such report to detect, investigate, and address international cybercrime occurring within its territory or through the use of its infrastructure, including, as appropriate, steps taken in cooperation with the United States or in international fora;

(v) the positions (including voting records) on matters relating to cybercrime in the General Assembly of the United Nations and other international bodies and fora of each country that is the subject of such report;

(vi) the response of the judicial system of each country that is the subject of such report with respect to matters—

(I) relating to international cybercrime affecting United States citizens or interests; or

(II) that have, in the opinion of the Secretary, a significant impact on United States efforts relating to international cybercrime, including responses to extradition requests; and

(B)(i) any significant direct financial support provided to, or support for the activities of, groups or organizations referred to in paragraph (1)(B) by the government of each country that is the subject of such report;

(ii) any significant training, equipment, or other in-kind support to such groups or organizations by such governments; and

(iii) sanctuary from prosecution given by any such government to the members of such groups or organizations who are responsible for the commission, attempt, or planning of a major cybercrime incident;

(C) to the extent practicable, complete statistical information regarding the economic, security, and health and safety impacts of international cybercrime on the United States; and

(D) an analysis, as appropriate, of trends in international cybercrime, including changes in tactics, techniques, and procedures, demographic information on cybercriminals, and other appropriate information.

(3) CLASSIFICATION OF REPORT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the report required under paragraph (1), to the extent practicable—

(i) shall be submitted in an unclassified form; and

(ii) may be accompanied by a classified annex.

(B) EXCEPTION.—If the Secretary of State determines that the submission of the information with respect to a foreign country under subparagraph (C) or (D) of paragraph (1) in classified form would make more likely the cooperation of the government of such foreign country, the Secretary may submit such information in classified form.

SEC. 1296. IMPOSITION OF SANCTIONS WITH RESPECT TO MAJOR CYBERCRIME INCIDENTS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and not less frequently than annually thereafter, the President shall—

(1) identify each foreign person that the President determines—

(A) knowingly engages in activities responsible for, or intended to cause, a major cybercrime incident;

(B) is owned or controlled by, or acts or purports to act for or on behalf of, directly or indirectly, a person described in subparagraph (A); or

(C) knowingly materially assists, sponsors, or provides financial, material, or technological support for, or goods or services in support of—

(i) an activity described in subparagraph (A); or

(ii) a person described in subparagraph (A) or (B), the property and interests in property of which are blocked pursuant to this section;

(2) except as provided under subsection (d), impose the sanctions described in subsection (b) with respect to each individual identified under paragraph (1); and

(3) except as provided under subsection (d), impose 5 or more of the sanctions described in subsection (c) with respect to each entity identified under paragraph (1).

(b) APPLICABLE SANCTIONS.—The sanctions referred to in subsection (a)(2) are the following:

(1) BLOCKING OF PROPERTY.—The President shall exercise all of the powers granted to the President under the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of any individual identified under subsection (a)(1) if such property or interests in property—

(A) are in the United States;

(B) come within the United States; or

(C) come within the possession or control of a United States person.

(2) INELIGIBILITY FOR VISAS, ADMISSION, OR PAROLE.—

(A) VISAS, ADMISSION, OR PAROLE.—Any alien identified under subsection (a)(1)—

(i) is inadmissible to the United States;

(ii) is ineligible to receive a visa or other documentation to enter the United States; and

(iii) is ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry document issued to any alien identified under subsection (a)(1) is subject to revocation regardless of when such visa or document was issued.

(ii) IMMEDIATE EFFECT.—The revocation of an alien's visa or other entry document pursuant to clause (i)—

(I) shall take effect in accordance with section 221(i) of the Immigration and Nationality Act (8 U.S.C. 1201(i)); and

(II) shall cancel any other valid visa or entry document that is in the alien's possession.

(c) ADDITIONAL SANCTIONS.—The sanctions referred to in subsection (a)(3) are the following:

(1) EXPORT-IMPORT BANK ASSISTANCE FOR EXPORT TO SANCTIONED PERSONS.—The President may direct the Export-Import Bank of the United States not to approve the issuance of any guarantee, insurance, extension of credit, or participation in the extension of credit, or participation in the extension of credit in connection with the export goods or services to any entity identified under subsection (a)(1).

(2) EXPORT SANCTION.—The President may order the United States Government not to issue any specific license, and not to grant any other specific permission or authority to export any goods or technology, to any entity identified under subsection (a)(1) under—

(A) the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.);

(B) the Arms Export Control Act (22 U.S.C. 2751 et seq.);

(C) the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.); or

(D) any other statute that requires the prior review and approval of the United States Government as a condition for the export or reexport of goods or services.

(3) LOANS FROM UNITED STATES FINANCIAL INSTITUTIONS.—The President may prohibit any United States financial institution from making loans or providing credits to an entity identified under subsection (a)(1) that totals more than $10,000,000 in any 12-month period unless—

(A) such entity is engaged in activities to relieve human suffering; and

(B) such loans or credits are specifically provided for such activities.

(4) LOANS FROM INTERNATIONAL FINANCIAL INSTITUTIONS.—The President may direct the United States executive director to each international financial institution to use the voice and vote of the United States to oppose any loan from the international financial institution that would benefit an entity identified under subsection (a)(1).

(5) PROHIBITIONS FOR FINANCIAL INSTITUTIONS.—The following prohibitions may be imposed against any entity identified under subsection (a)(1) that is a financial institution:

(A) PROHIBITION ON DESIGNATION AS PRIMARY DEALER.—Neither the Board of Governors of the Federal Reserve System nor the Federal Reserve Bank of New York may designate, or permit the continuation of any prior designation of, such entity as a primary dealer in United States government debt instruments.

(B) PROHIBITION ON SERVICE AS A REPOSITORY OF GOVERNMENT FUNDS.—Such entity may not serve as agent of the United States Government or serve as repository for United States Government funds.

(C) TREATMENT OF SANCTIONS.—For purposes of subsection (a)(3)—

(i) the imposition of a sanction under subparagraph (A) or (B) shall be treated as 1 sanction; and

(ii) the imposition of both sanctions under subparagraphs (A) and (B) shall be treated as 2 sanctions.

(6) PROCUREMENT SANCTION.—The United States Government may not procure, or enter into any contract for the procurement of, any goods or services from any entity identified under subsection (a)(1).

(7) FOREIGN EXCHANGE.—Pursuant to such regulations as the President may prescribe, the President may prohibit any transactions in foreign exchange that are subject to the jurisdiction of the United States and in which any entity identified under subsection (a)(1) has any interest.

(8) BANKING TRANSACTIONS.—Pursuant to such regulations as the President may prescribe, the President may prohibit any transfers of credit or payments between financial institutions or by, through, or to any financial institution, to the extent that such transfers or payments are subject to the jurisdiction of the United States and involve any interest of an entity identified under subsection (a)(1).

(9) PROPERTY TRANSACTIONS.—Pursuant to such regulations as the President may prescribe, the President may prohibit any person from—

(A) acquiring, holding, withholding, using, transferring, withdrawing, transporting, or exporting any property that is subject to the jurisdiction of the United States and with respect to which any entity identified under subsection (a)(1) has any interest;

(B) dealing in or exercising any right, power, or privilege with respect to such property; or

(C) conducting any transaction involving such property.

(10) BAN ON INVESTMENT IN EQUITY OR DEBT OF SANCTIONED PERSON.—Pursuant to such regulations or guidelines as the President may prescribe, the President may prohibit any United States person from investing in or purchasing significant amounts of equity or debt instruments of any entity identified under subsection (a)(1).

(11) EXCLUSION OF CORPORATE OFFICERS.—The President may direct the Secretary of State to deny a visa to, and the Secretary of Homeland Security to exclude from the United States, any alien that the President determines is a corporate officer or principal of, or a shareholder with a controlling interest in, any entity identified under subsection (a)(1).

(12) SANCTIONS ON PRINCIPAL EXECUTIVE OFFICERS.—The President may impose on the principal executive officer or officers of any entity identified under subsection (a)(1), or on persons performing similar functions and with similar authorities as such officer or officers with respect to such entity, any of the sanctions under this subsection.

(d) NATIONAL SECURITY WAIVER.—The President may waive the imposition of sanctions under this section with respect to a foreign person, if the President—

(1) determines that such a waiver is in the national security interests of the United States; and

(2) not more than 15 days after issuing such waiver, submits to the appropriate congressional committees a notification of the waiver and the reasons for the waiver.

SA 4242. Mr. MENENDEZ submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in title XII, insert the following:

SEC. _____. REPORT BY SECRETARY OF STATE ON FOREIGN MERCENARIES.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State, in consultation with the Director of National Intelligence and the Secretary of Defense, shall submit to the appropriate congressional committees a report on the extent to which foreign mercenaries are being used by countries to train, equip, advise, participate in, or conduct military, security, police, or intelligence-gathering activities and operations.

(b) ELEMENTS.—The report required under subsection (a) shall include the following elements:

(1) A description and evaluation of the use of foreign mercenaries, by country.

(2) A detailed description and evaluation of each such country's justification for the use of foreign mercenaries.

(3) The extent to which such foreign mercenaries are directly or indirectly sponsored or directed by the governments of their countries of origin.

(4) A description of any standards, laws, policies, or regulations that apply to the behavior of such mercenaries, including whether any judicial proceedings have been conducted against such mercenaries within the prior two years.

(5) An estimate of the number of United States citizens engaged in or suspected to be engaged in mercenary activities and operations, including the number of such citizens who have received an export license by the Department of State to engage in such activities or operations, disaggregated by foreign country in which such activities or operations have been authorized, including a description of any investigations that the Department has initiated or participated in concerning such citizens or any other United States citizen who has not received such an export license.

(c) FORM.—The report required under subsection (a) shall be submitted in unclassified and unredacted form, and not subject to any additional restriction on public dissemination, to the maximum extent feasible, but may include a classified, unredacted annex.

(d) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations, the Committee on Armed Services, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Foreign Affairs, the Committees on Armed Services, and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) MERCENARY.—The term ''mercenary'' means a person who—

(A) is not, as of the date on which the report required under subsection (a) is submitted, a member of the military, the security forces, or any law enforcement agency of the government of the country of which the person is a national; and

(B) is engaged in any military-, security-, or intelligence-related activity in a country of which such person is not a national and is not licensed or contracted for such activity by the Government of the United States.

SA 4243. Mr. MENENDEZ submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle E of title XII, add the following:

SEC. 1253. ESTABLISHMENT OF JOINT INTERAGENCY TASK FORCE ON USE OF GRAY-ZONE TACTICS IN THE INDO-PACIFIC MARITIME DOMAIN.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of State shall establish a joint interagency task force to assess, respond to, and coordinate with United States allies and partners in response to the use of gray-zone tactics by state and nonstate actors in the Indo-Pacific maritime domain.

(b) ACTIVITIES.—The task force established under subsection (a) shall—

(1) conduct domain awareness operations, intelligence fusion, and multi-sensor correlation to detect, monitor, disrupt, and deter suspected gray-zone activities;

(2) promote security cooperation and capacity building to respond to, disrupt, and deter gray-zone activities; and

(3) coordinate United States and partner country initiatives, including across diplomatic, political, economic, and military domains, to counter the use of gray-zone tactics by adversaries.

SA 4244. Mr. MENENDEZ submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title XII, add the following:

SEC. 1283. SECURITY IMPLICATIONS OF THE COUP IN SUDAN ON UNITED STATES SECURITY INTERESTS.

(a) REPORT.—

(1) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act, the Secretary of Defense, in consultation with the Secretary of State and the Director of National Intelligence, shall submit to the appropriate committees of Congress a report on the coup in Sudan on October 25, 2021.

(2) ELEMENTS.—The report required by paragraph (1) shall include the following:

(A) An assessment of the security implications of such coup for United States security interests in the Horn of Africa.

(B) An identification of any country that supported such coup.

(3) FORM.—The report required by paragraph (1) shall be submitted in unclassified form but may contain a classified annex.

(b) PROHIBITION ON ASSISTANCE.—

(1) IN GENERAL.—Amounts authorized to be appropriated by this Act, or any other Act, may not be obligated or expended to provide assistance to the Government of Sudan until the date on which the certification described in paragraph (2) is made.

(2) CERTIFICATION DESCRIBED.—The certification described in this paragraph is a certification by the Secretary of State to the appropriate committees of Congress that the following criteria have been met:

(A) The Prime Minister of Sudan, other civilian members of the Sovereign Council of Sudan, members of civil society, and other individuals detained in connection with the coup in Sudan on October 25, 2021, have been released from detention.

(B) Sudan has returned to constitutional rule under the transitional constitution.

(C) The state of emergency in Sudan has been lifted, including the full restoration of all means of communication.

(D) The military forces of Sudan, including the rapid support forces, have been ordered to return to their barracks.

(c) SANCTIONS.—The President shall immediately identify the leaders of the coup in Sudan on October 25, 2021, their accomplices, and foreign and United States persons that the President determines enabled the coup for the imposition of sanctions pursuant to applicable sanctions laws.

(d) OPPOSITION TO SUPPORT BY INTERNATIONAL FINANCIAL INSTITUTIONS.—The Secretary of the Treasury shall use the voice